DIVISIBILITY OF CLASS NUMBERS OF REAL QUADRATIC FIELDS(Analytic Number Theory and Surrounding Areas)

AUTHOR(S):

CHAKRABORTY, KALYAN

数理解析研究所講究録
1511 巻 2006 年 188-196

DIVISIBILITY OF CLASS NUMBERS OF REAL QUADRATIC FIELDS

KALYAN CHAKRABORTY

ABSTRACT. Class numbers of real quadratic fields have been the object of attention for many years and there exist a large number of interesting results. This is a survey article aimed at reviewing results concerning the divisibility of class numbers of real quadratic fields and specially regarding getting a lower bound on the number of real quadratic fields whose class number is divisible by a given integer and whose absolute discriminant is bounded by a large real number.

1. INTRODUCTION

Starting from Gauss, class numbers of quadratic fields have been studied extensively and thus there exist many interesting results. Here we would like to survey some results concerning the divisibility of class numbers of real quadratic fields. We will also provide a sketch of the proof proof of some results. This is by no means a complete survey of this field of research and thus misses many references and interesting results.

We consider the following two questions:

(1) Qualitative Direction : Given $g \geq 2$ an integer do there exist infinitely many real quadratic fields whose class number is divisible by g?

(2) Quantitative Direction. Derive a lower bound on the number of real quadraitc fields whose class number is divisible by a given integer and whose absolute discriminant is bounded by a large real number?

In the following let $d \geq 1$ be a square free integer and we consider the field $\mathbb{Q}(\sqrt{d})$. We let $h(d)$ denote its class number.

2. CLASSICAL RESULTS

The first question was answered in the "affirmative" by Y. Yamamoto in 1970 [20] and later by P. J. Weinberger in 1973 [17]. We would like to sketch the proof of Weinberger.

Theorem 1. *For all positive integers g, there exists infinitely many real quadratic fields with class numbers divisible by g.*

Weinberger considered discriminants of the type $d = n^{2g} + 4$ with $n > g$ a prime. Then the fundamental unit of $\mathbb{Q}(\sqrt{d})$ is $\frac{n^g+\sqrt{d}}{2}$ (of course one avoids $d = 5$). Now suppose that $T^k - 4$ is irreducible in $\mathbb{F}_n[T]$ for all $k|g$. In this set up one considers the ideal $\mathcal{A} = (n^2, 2+\sqrt{d})$. Clearly, the order of $\mathcal{A}$ in the class group of $\mathbb{Q}(\sqrt{d})$ is a divisor of g. Then it is not difficult to show that the order of $\mathcal{A}$ is exactly g or $g/2$ whenever g is odd or even respectively with the above assumptions. Here one uses the fundamental unit. Next one applies some density theorem (e.g. Chebotarev density theorem) to conclude that there exist infinitely many primes n such that $T^k - 4$ is irreducible in $\mathbb{F}_n[T]$ for all $k|g$.

Now repetations of the fields possible only when

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{n^{2g}+4}).$$

It is well known that the Diophantine equation $x^{2g} + 4 = Dy^2$ has only finitely many solutions. This implies that repetations of the resulting fields are possible only for finitely many n. This complets the proof of infinitude of such fields.

Remark 1. *Humio Ichimura* [9] *recently showed that the conditions assumed in Weinberger's proof are not necessary and proved that for all integers $n \geq 2$ and every odd integer $a \geq 3$, the ideal class number of $\mathbb{Q}(\sqrt{a^{2n}+4})$ is divisible by n.*

The corresponding result in case of imaginary quadratic fields was first established by Nagell [15] and later another elegant proof was provided by Ankeny and Chowla [1].

Now we move to question (2). Let us denote by

$$N_g(X) = \#\{d \leq X \ : \ g \mid h(d)\}$$

here X is a large real number. Thus the problem is to get a lower bound of $N_g(X)$ interms of X.

The famous Cohen - Lenstra heuristics [8] predict that quadratic fields (in fact for any number field of degree $n > 1$) with class number divisible by g should have positive density among all quadratic fields (all number fields of degree n). Thus the prediction is $N_g(X) \sim c_g X$ for a positive constant c_g. For odd primes g, it predicts

$$\begin{aligned} c_g &= \frac{6}{\pi^2}\Big(1 - \prod_{i=2}^{\infty}(1 - \frac{1}{g^i})\Big) \text{ (In the real case)} \\ &= \frac{6}{\pi^2}\Big(1 - \prod_{i=1}^{\infty}(1 - \frac{1}{g^i})\Big) \text{ (In the imaginary case).} \end{aligned}$$

This implies a positive proportion of quadratic fields contain a non-trivial p-part in the class group. So far very little progress has been made towards settling this conjecture.

R. Murty [14] was the first to consider getting a lower bound and he proved the following result.

Theorem 2.

$$N_g(X) \gg X^{\frac{1}{2g}-\epsilon}$$

for any $\epsilon > 0$ and g odd.

Murty quantified Weinberger's construction of discriminants. In Weinberger's proof we have,

$$n^{2g} + 4 = d \leq X \Rightarrow n < X^{\frac{1}{2g}}.$$

Further assumption is that n is a prime such that $T^k - 4$ is irreducible (mod n) for all $k|g$. Application of Chebotarev density theorem ensures that

$$\#\text{ of such } n \gg \frac{X^{\frac{1}{2g}}}{\log X}.$$

Weinberger showed that for each such n, the class group of $\mathbb{Q}(\sqrt{d})$ has an element of order g. The final step is to get an upper bound on the number of fields which are repetated by this construction. One needs to show that this estimate is smaller compared to the main estimate.

We need to count the number of integral solutions of the Diophantine equation $dy^2 = n^{2g} + 4$ for a fixed d. A result of Evertse - Silverman [5] concludes that the number of such n's can be atmost $C^{\nu(d)}$ for some absolute constant C. Here $\nu(d)$ represents the number of prime factors of d and a classical estimate of Ramanujan gives that

$$\nu(d) \ll \frac{\log d}{\log\log d}.$$

This complets the proof.

Remark 2. *(a) The above argument goes through for $g = 2r$, r is odd and one derives the same estimate. When $g = 4r$ one gets a weaker estimate than the above by this argument. The exponent $2g$ gets replaced by $4g$.*
(b) In the same paper Murty also gets the first non trivial bound of $N_g(X)$ in case of imaginary quadratic fields. He showed

$$N_g(X) \gg X^{\frac{1}{2}+\frac{1}{g}}.$$

Though Ankeny and Chowla [1] *did not mention it, their method (in case of imaginary quadratic fields) demonstrates that*

$$N_g(X) \gg X^{\frac{1}{2}}.$$

3. Recent improvements of Murty's real bound

Recently, Gang Yu [7] used Yamamoto's construction [20] of discriminants (needs to have two different representations of each discriminants by a special binary polynomial) and by quantifying it, he could improve Murty's real bound. Yu showed,

Theorem 3. *Let g be odd. Then for any $\epsilon > 0$*

$$N_g(X) \gg X^{\frac{1}{g}-\epsilon}.$$

We would like to sketch his proof. Let $g = p_1^{\delta_1} \cdots p_k^{\delta_k}$ with distinct primes. For all p_j, fix two primes l_j and l_j' such that $l_j \equiv l_j' \equiv 1 \pmod{p_j}$ and 2 is a p_j-th power $\pmod{l_j}$ and 3 is not. Set

$$\alpha = \prod_{j=1}^{k} l_j' \; \beta = \prod_{j=1}^{k} l_j', \; \Omega = 4\alpha\beta.$$

Then the following useful result of Yamamoto provides the shape of d such that $g \mid h(d)$.

Lemma 1. *For a, b two positive integers satisfying*

$$a \equiv \alpha \pmod{\Omega}, b \equiv \beta \pmod{\Omega}.$$

Let

$$d = \frac{3}{4}(3a^g + b^g)(a^g + 3b^g).$$

Then $g \mid h(d)$.

Thus if $f(a,b) = (3a^g + b^g)$ and $F(a,b) = f(a,b)f(b,a)$, then the target is to estimate the number of a, b which are represented by $F(a,b)$ in a range which satisfy some additional restrictions and by estimating that he gets his bound.

Later, F. Luca [6] derived the same estimate as that of Yu in case when g is odd. He adopted an entirely differnt method. He showed,

Theorem 4. *Let $G = l.c.m[g, 2]$, then*

$$N_g(X) \gg \frac{X^{\frac{1}{g}}}{\log X}.$$

Let $Y = X^{\frac{1}{2g}}$ and

$$P = \{ \text{ odd primes } p \leq X : x^G - 2 \text{ irreducible } \pmod{p}\}.$$

Now $|P| \gg \frac{X^{\frac{1}{G}}}{\log X}$. One writes $p^G + 1 = dz^2$ for all $p \in P$. Clearly, $d < X$ and 2 exactly divides d. Now one ignores the p's which contribute to the case $d = 2$, as this does not reduce the estimate.

Now one would like to show that the d's thus appearing from $p \in P$ (such that $d \neq 2$) are mutually distinct and for every one of these d's one has $G|h(d)$.

Consider the Pell Equation $x^2 - dy^2 = -1$. The pair of integers $(x, y) = (p^{\frac{G}{2}}, z)$ is a solution of this equation. Let (x_m, y_m) stand for the m-th solution for some integer m. Now, Pell equation theory confirms that $p^{\frac{G}{2}} = x_m$ should hold for some odd integer m. One shows infact that $m = 1$. Thus $\zeta = p^{\frac{G}{2}} + z\sqrt{d}$ is the fundamental unit in the ring of integers of $\mathbb{Q}(\sqrt{d})$. This proves that all the resulting fields are mutually distinct.

Finally it is not difficult to produce an element of order G in the class group.

4. Improvement in case when $g = 3$

In a recent work the present author alongwith R. Murty [13] has the following improvement in case when $g = 3$.

Theorem 5.

$$N_3(X) \gg X^{\frac{5}{6}}.$$

One considers polynomials of the type $f(x) = x^3 + ax + b$. Denote the discriminant of f as $D(f)$ and that equals $-(4a^3 + 27b^2)$ and F as splitting field of f. It is well known that if $f(x) \in \mathbb{Z}[x]$ is irreducible and $d(f)$ is not a square then the Galois group of F over $\mathbb{Q}$ is S_3. Next one gets the following estimate

$$\#\{|a| \leq A, |b| \leq B : f(x) \text{ is irreducible and} D(f) \text{ is not a square}\} \gg AB.$$

If in the above situation one further assumes $(2a, 3b) = 1$, then a result of Yamamoto [20] says that F is unramified over $\mathbb{Q}(\sqrt{d})$. Thus its Galois group is C_3. Now by class field theory F is contained in Hilbert class field of $\mathbb{Q}(\sqrt{D(f)})$. Hence $3|h(D(f))$. Now to make $D(f)$ positive we consider a large negative and b positive. Thus consider

$$-c_1 X^{\frac{1}{3}} < a \leq -c_2 X^{\frac{1}{3}} \ , \ c_3 X^{\frac{1}{2}} < b \leq c_4 X^{\frac{1}{2}}$$

for suitable constatnts c_i's for $i = 1, \cdots, 4$.

Thus one has $X^{\frac{1}{3}}$ choices of a's and $X^{\frac{1}{2}}$ choices of b's, and so one has $X^{\frac{5}{6}}$ choices of such fields.

Finally one has to show there are very few repetations. If S be the set of $D(f)$'s above which give rise to same fields more than once, then it follows that $\#S = O(X^{\frac{2}{3}+\epsilon})$. Thus there exists

$$\gg X^{\frac{5}{6}} - O(X^{\frac{2}{3}+\epsilon})$$

distinct fields, which proves the result.

K. Soundararajan [16] improved Murty's imaginary bound. He showed,

Theorem 6.

$$\begin{aligned} \text{For } 4|g \ , \ N_g(X) &\gg X^{\frac{1}{2}+\frac{2}{g}-\epsilon} \\ \text{For } 4|(g-2) \ , \ N_g(X) &\gg X^{\frac{1}{2}+\frac{3}{g+2}-\epsilon} \end{aligned}$$

for any $\epsilon > 0$.

Soundararajan's result contains an improvement for odd g too as $N_g(X) \geq N_{2g}(X)$. In particular it says that when $g = 3$,

$$N_3(X) \gg X^{\frac{7}{8}-\epsilon}.$$

Recently, D. Byeon and E. Koh [4] further improved the real bound in the case when $g = 3$. They used the above imaginary bound of Soundararajan and a different characterization of real quadratic fields which has an element of order 3 in its class group. This characterization is due to Y. Kishi and K. Miyake [21]. Byeon and Koh showed

Theorem 7.

$$N_3(X) \gg X^{\frac{7}{8}}.$$

5. CONCLUDING REMARKS

A lot more work has centered around the complementary question of finding class groups whose order is not divisible by a given g. A beautiful work of W. Kohnen and K. Ono [18] proves the existence of at least $\sqrt{X}/\log X$ imaginary quadratic fields with absolute discriminant is bounded by a large real X and $l \not| h(d)$ for a given prime l. A similar bound is obtained by K. Ono [10] in case of real quadratic fields. One can collect work done in this direction from a recent survey article by W. Kohnen [19].

Much less is known for fields of higher degrees. The best result so far is the recent work of Y. F. Bilu and F. Luca [22]. They proved

Theorem 8. *Let n and l be positive integers with $n \geq 2$. Put $\mu = \frac{1}{2(n-1)l}$. There exist positive real numbers $X_0 = X_0(n,l)$ and $c = c(n,l)$ such that for any $X > X_0$, there is at least cX^{μ} pairwise non-isomorphic number fields of degree n, discriminant less than X and class number is divisible by l.*

In principle all these results should be generalized to the function field set up. A quadratic function field $K = \mathbb{F}_q(t, \sqrt{D})$ is said to be real if infinity splits completely in K and it is imaginary otherwise. C. Friesen [2] proved the existence of infinitely many such real quadratic function fields whose class numbers are divisible by a given positive integer. The present author in a joint work with A. Mukhopadhaya [11] quantified Friesen's method.

Theorem 9. *Let q be a power of an odd prime and $g \geq 3$ be a given integer. Then there exist $\gg q^{\frac{l}{2g}}$ real quadratic extensions $\mathbb{F}_q(t, \sqrt{D})$ of the rational function field $\mathbb{F}_q(t)$ such that degree of D is $\leq l$ and ideal class number of $\mathbb{F}_q(t, \sqrt{D})$ is divisible by g.*

By generalizing F. Luca's method [6] in case of function fields over finite fields the present author in another joint work with A. Mukhopadhaya [12] improved the above bound to

$$\gg \frac{q^{\frac{l}{g}}}{l^2}.$$

In case of imaginary quadratic function fields R. Murty and D. Cardan [3] showed that there are

$$\gg q^{l(\frac{1}{2}+\frac{1}{g})}$$

imaginary quadratic extensions $\mathbb{F}_q(t, \sqrt{D})$ with degree of D is bounded by l and whose ideal class group has an element of order g. All these results are far away from the actual prediction of Cohen and Lenstra. May be one needs a completely different approach to the problem to settle the conjecture.

Acknowledgement: The author wishes to express his heartful thanks to Prof. Katsuya Miyake for sponsoring his trip to Japan and for being a wonderful host in Japan.

References

[1] N. Ankeny and S. Chowla : On the divisibility of the class numbers of quadratic fields, *Pacific Journal of Math.*, **5** (1955), 321–324. MR **19**:18f

[2] Christian Friesen : Class number divisibility in real quadratic function fields, *Canad. Math. Bulletin*, **32** (1992), no. 3, 361–370. MR **93h**:11130.

[3] David A. Cardon and M. Ram Murty : Exponents of class groups of quadratic function fields over finite fields, *Canadian Math. Bulletin*, **44** (2001), 398–407.

[4] Dongho Byeon and Eunhee Koh : Real quadratic fields with class number divisible by 3, *Manuscripta Math.*, **111** (2003), no. 2, 262–263.

[5] J.H. Evertse and J.H. Silverman : Uniform bounds for the number of solutions to $Y^n = f(x)$, *Math. Proc. Camb. Phil. Soc.*, **100** (1986), 237–248.

[6] Florian Luca : A note on the divisibility of class numbers of real quadratic fields, *C. R. Math. Acad. Sci. Soc. R. Can.*, **25** (2003), 71–75.

[7] Gang Yu : A note on the divisibility of classs numbers of real quadratic fields, *J. Number Theory*, **97** (2002), no. 1, 35–44.

[8] H. Cohen and H. W. Lenstra Jr. : Heuristics on class groups of number fields, *Springer Lecture Notes*, **1068** in Number Theory Noordwijkerhout 1983 Proceedings. MR **85j**: 11144

[9] Humio Ichimura : Note on the class numbers of certain real quadratic fields, *Abh. Math. Sem. Univ. Hamburg*, **73** (2003), 281–288.

[10] Ken Ono : Indivisibility of class numbers of real quadratic fields, *Compositio Math.*, **119** (1999), no.1, 1–11.

[11] Kalyan Chakraborty and Anirban Mukhopadhyay : Exponents of class groups of real quadratic function fields, *Proc. Amer. Math. Soc.*, **132**, No. 7, 1951–1955.

[12] Kalyan Chakraborty and Anirban Mukhopadhyay : Exponents of class groups of real quadratic function fields II, *To appear in Proc. Amer. Math. Soc.*.

[13] K. Chakraborty and M. Ram Murty : On the number of real quadratic fields with class number divisible by 3, *Proc. Amer. Math. Soc.*, **131**. no. 1, 41–44.

[14] M. Ram Murty : Exponents of classs groups of quadratic fields, *Topics in Number Theory (University Park, PA, 1997), Math. Appl.*, **467**, *Kluwer Acad. Publ., Dordrecht*, (1999), 229–239. MR **2000b**:11123.

[15] T. Nagell : Uber die Klassenzahl imaginar quadratischer, *Zahlkorper, Abh. Math. Sem. Univ. Hamburg*, **1** (1922), 140–150.

[16] K. Soundrarajan : Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.*, **61** (2000), no. 2, 681–690. MR **2001i**:11128.

[17] P. Weinberger : Real quadratic fields with class number divisible by n, *J. Number Theory*, **5** (1973), 237–241. MR **49**:252.

[18] Winfried Kohnen and Ken Ono : Indivisibilty of class numbers of imaginary quadratic fields and orders of Tate-Shafarvich groups of elliptic curves with complex multiplication, Invent. Math., **135** (1999), no. 2, 387 – 399.

[19] Winfried Kohnen : Class numbers of imaginary quadratic fields, *Class fields Theory - its centenary and prospect (Tokyo, 1998)*, 415–417, *Adv. Stud. Pure Math.*, **30**, Math. Soc. Japan, Tokyo, 2001.

[20] Y. Yamamoto : Galois extensions of quadratic number fields, *Osaka J. Math.*, **7** (1970), 57–76. MR **42**:1800.

[21] Yasuhiro Kishi and Katsuya Miyake : Parametrization of the quadratic fields whose class numbers are divisible by 3, *J. Number Theory*, **80** (2000), no. 2, 209–217.

[22] Yuri. F. Bilu and Florian Luca : Divisibilty of class numbers: enumerative approach, *To appear in Compositio Math.*

HARISH-CHANDRA RESEARCH INSTITUTE, CHHATNAG ROAD, JHUNSI, ALLAHABAD-211019, INDIA
E-mail address: kalyan@mri.ernet.in